UNITED STATES PATENT APPLICATION

FOR

SECURED ACCESS USING A COORDINATE SYSTEM

BY

CHRISTER FÅHRAUES, PETTER ERICSON

AND

SVEN OLOF KARLSSON

Cross-Reference to Related Applications

[001] This application claims priority benefits based on Swedish Patent Application No. 0000942-3, Filed March 21, 2000, and U.S. Provisional Application 60/207,850, filed May 30, 2000, the technical disclosures of both of which are hereby incorporated herein by reference.

Field of the Invention

[002] The present invention relates to systems for and methods of controlling a user's access to an access-protected unit.

Background of the Invention

[003] To protect different types of systems and devices, such as computers or other electronic equipment, against use by unauthorized individuals, it is known to equip them with some type of access protection. Typical computer access protection includes a user log in. To log in, the user typically enters a user identity and password which checks this information against information stored earlier in order to determine if the user is authorized to use the computer. The disadvantage of this process is that a user must memorize a password which can be difficult since we surround ourselves with many systems which demand a log in process and since these often have different passwords. Many users write down their password, with the consequence that if someone finds the record this person can gain unauthorized access into the system. If the user also has the same password for several different systems, this can have far-reaching consequences.

[004] In the Japanese document JP10222241 "Electronic Pen and System and Method for Individual Authentication", an electronic pen is described which is equipped with a gyrosensor. When a user writes his signature, the pen senses features of the signature and produces a password by means of an algorithm.

[005] It is also known from WO 99/48268 to replace the PIN code in a mobile communication unit with a signature which the user writes with the communication unit. The communication unit is equipped with a sensor of the gyrosensor or pressure-ball type which senses the movement when the user is writing with the unit.

[006] One problem of the above-mentioned techniques is that a signature is not difficult to forge.

Summary of A Few Aspects of the Invention

[007] The invention provides a method for controlling access to an access-protected unit. At least one pair of coordinates may be read from a base. If the pair of coordinates are within a coordinate area belonging to an authorized user, access to the protected unit may be granted.

[008] Also, the invention provides a system for controlling a user's access to an access-protected unit. The system may include a user unit for reading at least one pair of coordinates, and a checking device for checking, on the basis of the pair of coordinates, if the user is authorized to access the access-protected unit. If so, the system provides an enabling signal to the access-protected unit.

[009] The invention may also include a checking device for checking a user's access to an access-protected unit. The checking device may include memory for storing information about at least one coordinate area, and a processor. The processor

may be operative to receive at least one pair of coordinates and check, on the basis of the coordinates, if the user is authorized to access the access-protected unit. If so, the system may provide an enabling signal to the access-protected unit.

[010] The invention may also include a computer-readable medium containing instructions for controlling access to an access-protected unit. The instructions may include reading at least one pair of coordinates from a base; checking if the pair of coordinates are within a coordinate area belonging to an authorized user; and granting access to the authorized user if the coordinates are within the coordinate area belonging to the authorized user.

[011] The foregoing summarizes only a few aspects of the invention and is not intended to be reflective of the full scope of the invention as claimed. Additional features and advantages of the invention are set forth in the following description, may be apparent from the description, or may be learned by practicing the invention. Moreover, both the foregoing general description and the following detailed description are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

Brief Description of the Drawings

[012] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments of the invention and together with the description, serve to explain the principles of the invention.

[013] The invention will be described in greater detail in the text which follows, by means of embodiments and referring to the accompanying drawings, in which

[014] Fig. 1 illustrates a system consistent with a first embodiment of the present invention, comprising a digital pen and a coordinate base.

[015] Fig. 2 illustrates a system consistent with a second embodiment of the present invention, comprising a user unit and a log in card.

[016] Fig. 3 schematically illustrates a storage structure for storing, among other things, checking information in a checking device which is used in a system consistent with an embodiment of the present invention.

[017] Figure 4 illustrates a flow chart of a method consistent with an embodiment of the present invention.

[018] Fig. 5 illustrates a rules coordinate table consistent with an embodiment of the present invention.

Description of the Preferred Embodiments

[019] The invention may employ the concept of using a new parameter, namely coordinates, as a basis for checking the access to an access-protected unit. An advantage of a system which is based on coordinates is that, as will be seen below, it can be constructed with varying degrees of security, from a very simple system where it is enough to register a correct pair of coordinates, to a very secure system where both, for a given embodiment, a correct pair of coordinates and a correct signature and/or the identity of the user must be registered.

[020] Coordinates may be suitable for being used as a basis for access control in any number of situations, but may have additional benefits when the access-protected unit lacks a keyboard, since coordinates can be registered by being read with a sensor.

[021] For example, the coordinates can be registered by the user unit optically reading a position-coding pattern which codes coordinates for a plurality of points. Access to an access-protected unit can then be obtained by the user registering coordinates for points within a particular coordinate area.

[022] Coordinates may also be suitable for use as parameters for access-control in systems for electronic registration of handwriting since handwritten text which is written on a writing surface with position-coding patterns can be registered electronically as a sequence of coordinates by continuous reading of the position-coding pattern. Position-coding patterns which can be used for registering handwritten text are described in, for example, US 5,852,434 and Applicants' patent applications WO 00/73983, PCT/SE00/01895 and WO 01/16691, the technical disclosures of which are incorporated herein by reference. The position-coding patterns described in Applicants' patent applications above can code coordinates for a very large number of positions on an imaging surface. Different coordinate areas can then be allocated to different users and the position-coding pattern which corresponds to the coordinate area can be imaged on a personal card or the like allocated to the user. The user can access a certain access-protected unit by reading coordinates from this card.

[023] The access-protected unit is a unit which is to be protected from unauthorized persons. Examples of access-protected units are computers, buildings, vehicles, web pages and different types of electronic equipment.

[024] In one embodiment of the system according to the invention, the checking device may be arranged to check if the coordinates are lying within a predetermine coordinate area for checking the authorization of the user.

[025] As a very simple example, a hand-held scanner or digital pen can be envisaged for electronic registration of handwriting, where the owner can only log in by registering coordinates from a card obtained with the purchase of the scanner/pen. In this case, the checking device may be located in the scanner/pen and may only need to have information on the extent of the predetermined coordinate area and to check that the registered coordinates are lying within this field.

[026] Log in on different scanners/pens can require coordinates from different coordinate areas.

[027] The coordinate area may be defined in advance and can, for example, be defined as lying within determined coordinates which represent the corners of the field.

[028] In an alternate embodiment of the system, the user unit is arranged to register a user signature as a sequence of coordinates which describe the displacement of the user unit when a user is writing the user signature with the user unit and where at least one pair of coordinates comprise the sequence of coordinates.

[029] An advantage of the user writing his signature is that the security may be increased. The signature may be the signed name of the user but can also be a symbol or any type of sign. For an unauthorized person to be able to log in to the access-protected unit, both access to the coordinate area and signature of the authorized user may be required in this case. This higher security can be implemented without the hardware of the system needing to be changed, since registration of the signature and registration of the coordinates can be done with the same technology.

[030] The checking device may be suitably arranged to compare the sequence of coordinates which thus represent the registered signature, with a sequence of coordinates stored earlier for checking the authorization of the user. The enabling signal for the access-protected unit may only be given if the sequences correspond to the desired extent. As used herein, when correspondence is detected the sequence of coordinate pairs are said to "favorably compare" with the stored sequence.

[031] In one embodiment of the system, the user unit may have a unique identification code and the checking device may be arranged to check authorization of the user with the identification code in combination with at least one pair of coordinates.

[032] By checking not only the coordinates but also the identification code, the security of the system will increase. If, for example, the coordinates are imaged on a card and this card is stolen, the thief cannot have access to the access-protected unit without the associated user unit. The identification code can be an identification number, such as a PIN (Personal Identification Number), a symbol, or any type of sign.

[033] In another embodiment of the system, the user unit may be arranged to register a sequence of coordinates which are associated to a specific access-protected unit.

[034] For example, the user can write different commands with the user unit and the user unit may then register this as sequences of coordinates. Depending on what commands the user is writing different access-protected units can be enabled. In this way the user can use the same equipment to log in to different physical units.

[035] The user unit, the checking device and the access-protected unit can be physically placed in different ways with respect to one another.

[036] The checking device can be physically integrated with the user unit, with the access-protected unit, or be self-contained. The checking device can also be physically divided, which implies that a certain part of the authorization check is done in one place and another part of the authorization check is done in another place. For example, a first check can be done in the user unit and a second check in the access-protected unit.

[037] When the checking device is self-contained, it can be used jointly for a plurality of user units and a plurality of access-protected units. It then may become more complicated and need to have a greater memory and processing capacity, among other things.

[038] When the checking device is integrated with the user unit, it may only need to check users of the access-protected unit or units which can be accessed via the user unit.

[039] In another embodiment of the system, the access-protected unit may be integrated with the user unit. The access may then apply to the user unit itself. The user unit and the access-protected unit can, therefore, be one and the same unit. In this case, the user may start the unit and may then log in, during which she may only use the functions of the unit which are required for log in, i.e., registration of coordinates and possibly other log in parameters. The functions which may be accessible during log in can be said to correspond to the user unit, while the remaining functions which may become accessible only after correct log in can be said to correspond to the access-protected unit.

[040] The checking device can be integrated with the user unit and the access-protected unit.

[041] As an alternative, the access-protected unit can be isolated from the user unit. It can be integrated with the checking device.

[042] In another embodiment of the system, the access-protected unit may be a digital pen which can be used for digitizing handwritten text.

[043] As already mentioned, the checking device can be common to a number of user units which may send the registered coordinates to the checking device. In this embodiment of the system, the information stored in the checking device may relate to a plurality of coordinate areas. The checking device can be, for example, web-based and reached via a computer network.

[044] Each coordinate area can be associated with one or more users and/or one or more access-protected units. In the former case, a number of users can thus reach a unit by registering coordinates from one and the same predetermined field. This can be desirable, for example, if the access-protected unit is a computer which a number of persons are to be able to use, or premises to which a number of persons are to be able to gain entry. In the latter case, for example, a person can access different access-protected units by registering coordinates from one and the same predetermined coordinate area. For example, a person may be permitted to log in to different apparatuses via a standard log in process.

[045] In one embodiment of the system, if the user is authorized to access the access-protected unit, the access-protected unit may be arranged to start at least one function associated with at least one of the plurality of coordinate areas.

[046] One advantage with this is that it may save the user time when logging in to an access-protected unit. The user can initially decide which functions he wishes to start when he is logging in. This set up can be changed when the user is logged in. Functions include different kinds of applications and programs.

[047] In another embodiment of the system, the access-protected unit may be associated with at least one of a plurality of coordinate areas.

[048] The coordinates may be registered by the user unit control for which access-protected unit the access is intended. This may result in a simple and flexible way of obtaining access to a certain access-protected unit. Different coordinate areas can be associated with different access-protected units. A coordinate area can also be associated with more than one access-protected unit, but then the user may need to indicate in some way which access-protected unit he wishes to access.

[049] In another embodiment of the system, there may be at least one authorized user identity which is associated with at least one of a plurality of coordinate areas.

[050] The coordinates which are registered by the user unit may control the user identity. Within the coordinate area which is associated with at least one authorized user, there can also be subareas which are associated with different access-protected units. The advantage of this is that if someone can forge a signature, he must also have access to the base with the predetermined coordinates which are associated with the signature.

[051] In another embodiment, the system may include a base provided with a position-coding pattern which enables coordinates to be determined and from which the user unit is arranged to register at least one pair of coordinates.

[052] Different coordinates are registered depending on where on the base the user places the user unit. The coordinates can be allocated different meanings. The base can be divided into different coordinate areas in which the user writes his signature or only places the user unit. Depending on which coordinate area the user is selecting, for example, access to different units can be carried out. This results in a quick and flexible activation of the access-protected unit for the user.

[053] In another embodiment, the user unit may include an optical sensor and image processor for registering at least one pair of coordinates.

[054] The optical sensor may obtain images and the image processor may process the images, determining the coordinates from the content of the images, which may be the above-mentioned position-coding pattern.

[055] The invention may also provide a checking device for checking a user's access to an access-protected unit, information about at least one coordinate area being stored in the checking device, the checking device being arranged to receive at least one pair of coordinates from a user unit which belongs to the user. The invention may then check, on the basis of the received coordinates, if the user is authorized to access the access-protected unit and, if so, to provide an enabling signal to an access-protected unit.

[056] The invention may also include a method for controlling access to an access-protected unit with the aid of a user unit, including the steps of registering at

least a pair of coordinates from a base using the user unit, checking with the checking device and on the basis of the registered coordinates, if the user is authorized to access the access-protected unit, and, if so, providing an enabling signal to the access-protected unit.

[057] According to another aspect of the invention, a method may be provided for checking authorization to an access-protected unit comprising receiving at least one pair of coordinates from a user unit which belongs to a user, checking on the basis of the received coordinates if the user is authorized to access the access-protected unit, and if so, providing an enabling signal to the access-protected unit.

[058] The invention may also provide a computer program which is stored on a computer-readable storage medium which includes instructions for causing the computer to carry out methods described above.

[059] The invention may further permit use of a position-coding pattern which codes coordinates for controlling access to an access-protected unit.

[060] In the text which follows, two exemplary schemes are described for implementing the invention. The first relates to access to a digital pen. The second relates to access to a computer. In the first scheme, the system for controlling access to the digital pen may be integrated with the digital pen. In the second scheme, the system for access control may be separate from the access-protected unit, i.e. the computer.

[061] Fig. 1 shows a digital pen 1 and a coordinate base 5. The digital pen 1 can be used as a normal writing pen, with a difference being that the text which is written can be recognized in digital form in the pen. To protect the pen against

unauthorized users, it may be provided with a system for controlling access to it (a log in system).

Log In Card

[062] Fig. 1 shows an embodiment of a log in card 5 which in this case may be similar to a normal magnetic or credit card with respect to size and material. The log in card 5, which may have a size of 10 mm x 200 mm, may include a writing field 6 provided with coordinates which can be read by the digital pen 1. The coordinates can be specified in explicit or coded form. In this embodiment, the log in card 5 may be provided with coordinates which are coded with the aid of a position-coding pattern 7. The pattern 7 is shown schematically as a number of dots on a part of the log in card 5.

[063] The writing field 6 may be intended for the user's signature. The log in card may also be made of a material permitting the signature to be erased after having been written. As an alternative, the combination of pen and log in card can be such that no pigment is deposited on the log in card when the user is writing the signature.

[064] The position-coding pattern 7 may have the characteristic that, if an arbitrary part of the pattern is registered with a certain minimum size, its position in the position-coding pattern and thus the log in card 5 may be determined unambiguously.

[065] The position-coding pattern 7 can be of the type shown in US 5,852,434, incorporated herein by reference, where each position is coded by a specific symbol.

[066] However, the position-coding pattern 7 may alternatively and advantageously be of the type shown in Applicants' above-mentioned Applications WO 00/73983, PCT/SE00/01895 and WO 01/16691, where each position may be coded by a plurality of symbols and each symbol may contribute to the coding of a number of

positions. The position-coding pattern 7 may be built up of a small number of types of symbols. An example is shown in WO 00/73983, where a larger dot represents a "one" and a smaller dot represents a "zero". Another example is shown in PCT/SE00/01895 and WO 01/16691, where four different displacements of a dot in relation to a raster point code four different values.

Digital Pen

[067] The digital pen 1 in Fig. 1 may include a casing 11. The short side of the casing may have an opening 12.

[068] The casing may include an optical part, an electronic part and a power supply.

[069] In the exemplary embodiment, the optical part may include at least one light-emitting diode 13 for illuminating the surface which is to be imaged and a light-sensitive area sensor 14, for example a CCD or CMOS sensor, for registering a two-dimensional image. The pen may also contain a lens system.

[070] The power supply for the pen may be obtained from a power source, such as a battery 15 which may be mounted in a separate compartment in the casing 11.

[071] The electronic part may contain a processor 16 which may be programmed for recording an image from the sensor 14, identifying symbols in the image, determining which pair of coordinates the symbols are coding and storing these coordinates in its memory. The processor 16 may also be programmed for analyzing the stored pairs of coordinates and converting them to a polygon train which constitutes a description of how the user unit is displaced over a surface provided with the position-

coding pattern, which displacement, for example, can represent the user's signature or some other form of handwritten information.

[072] The pen 1 also may comprise a pen point 17 with the aid of which the user can write normal pigment-based writing which, at the same time as it is written, is registered digitally by the pen 1 with the aid of the position-coding pattern. The pen point 17 can be retracted and extended so that the user can control if it is to be used or not. As used herein, the pen point generally refers to any marking or writing element regardless of whether it uses pigment, ink, or other marking material.

[073] The pen 1 may also include buttons 18 with the aid of which the unit may be activated and controlled. It also may have a transceiver 19 for wireless communication, for example by IR light or radio waves (e.g. BLUETOOTH), with external units.

Log In with the Aid of the Pen

[074] As mentioned, the pen 1 may be provided with a log in system. When the pen is switched on, it may be configured to require the user to log in prior to use. To handle the log in, the pen 1 may be provided with a log in program. Moreover, information regarding at least the user's specific coordinate area may be stored in the memory.

[075] In a first example, the access-unit may be the digital pen 1 which may also include a checking device having a memory in which coordinate areas and associated user identities are stored. Several users can have authorization for the pen 1. Each user can have his or her own log in card 5. The log in card 5 can be a card which the user carries, for example, in a wallet. When a user wishes to log in to the

digital pen 1, she may place it on the writing field 6 of the log in card 5, which may be provided with a position-coding pattern 7 unique to the user. A part of the pattern may be recorded optically by the digital pen 1. A program may convert the pattern into coordinates which are transferred to the checking device. The checking device may then check that the coordinates are within a predetermine coordinate area belonging to an authorized user. If so, the user may obtain access to the functions of the digital pen 1.

[076] Different users may have different coordinate areas, which may make it possible to control the programs to which different users are able to gain access by the pen, starting a different program depending on the coordinate area.

[077] To increase security on log in, it may be required that a user writes his signature in the writing field. The signature may be transferred to the checking device as a sequence of coordinates. The checking device may also check, in addition to the field within which the coordinates are located, if the sequence of coordinates for this coordinate area corresponds to an authorized sequence stored in the memory. As used herein, when correspondence is detected the sequence of coordinate pairs are said to "favorably compare" with the stored sequence. Thus, it may not be enough that an unauthorized person obtains the writing base and pen, but the unauthorized person must also be able to forge the signature of the authorized user in order to gain access to the functions of the pen.

Log In to Computer

[078] Fig. 2 shows a second embodiment of the invention, in which the access-protected unit is a computer 4, the user unit is a digital pen 1 and the checking device is

available on the web in the form of a server unit 2. The server unit 2 may handle a plurality of digital pens 1 and a plurality of computers 4.

[079] The digital pen 1 may be arranged to transfer information which is generated by the user to the server unit 2. While the information may be transmitted by a conventional hard-wired interface, in this embodiment the information may be transferred wirelessly to a network-access unit 8 by a wireless communication interface, such as a Bluetooth or IRDA interface, which, in turn, may transfer the information to the server unit 2. The network-access unit 8 may be a mobile telephone in this embodiment. As an alternative, it can be a computer or some other suitable unit which has an interface with a network, such as the Internet or a local company network. As an alternative, the network-access unit can constitute an integrated part of the user unit, e.g. digital pen 1.

[080] The server unit 2 may be a computer in a network of computers. It may be constructed as a traditional server unit with one or more processors, memory of different types, peripheral units and couplings to other computers in the network, but it has new software for carrying out the functions described herein. It may also have information stored in its memory in order to be able to handle these functions.

[081] In the memory of the server unit 2, information on the coordinate areas may be stored. The coordinate areas can be of different size and have different shape. A rectangular coordinate area, as exemplified in this embodiment, can be described with the aid of pairs of coordinates which represent points in the corners of the coordinate area. The writing field 6 on the log in card 5 may occupy one coordinate area.

[082] Information or rules for each coordinate area may be found in a data structure in the memory of the server unit 2. The information or rules may define how the information which can be associated with the coordinate area is to be processed.

[083] Fig. 3 shows an embodiment of such a structure in table form. In a first column 30 of the table, the coordinate areas are defined with the aid of the coordinates (x1,y1; x2,y2; x3,y3; x4,y4) for the corners of the coordinate area which have been assumed to be rectangular in this case. In a second column 31, a representation of the signature of the authorized user is stored so that the server unit 2 can compare a received signature with a signature stored earlier. As used herein, when correspondence is detected the sequence of coordinate pairs are said to "favorably compare" with the stored sequence. In a third column 32, a user identity may be stored in the form of a serial number for the user unit 1 of the authorized user. Naturally, this is a very simple structure which is only used for illustrating the principles of the invention. Considerably more complex structures and rules for security checking are conceivable within the scope of the invention.

[084] Figure 4 illustrates a flow chart of a method consistent with the present invention. At step 100, when a user wishes to obtain access to a computer 4, the user may place the digital pen 1 on the writing field 6 and the pen 1 may register the pattern 7 and calculate corresponding coordinates. The coordinates, together with a user identity stored in the user unit 1, may be forwarded via the mobile telephone 8 to the server unit 2. The server unit 2 may check to which coordinate area the registered coordinates belong. Each computer 4 in the system may be associated with at least one coordinate area. The server unit 2 may determine in this way for which computer

the access is intended. At step 110, the server unit 2 may then check that the user identity has the authority to log in to the computer for which the log in is intended. At step 120, if the user has authority, a signal may be sent to the computer 4 for which the access is intended, which may result in the user now being logged in to the computer 4. It is possible to send along special information from the server unit to a specific computer 4. This special information can comprise user-specific information which, in an exemplary embodiment, may start programs specific to the user. It can also be that different users obtain access to different amounts of information on the computer 4, which has the result that only certain parts of the content of the computer 4 may be opened up to the user. If the user does not have authorization for the computer 4, a message about this can be sent to the digital pen 1.

[085] To increase the security in the system, the user may also write his signature on the writing field 6 of the log in card 5. The signature may be registered as a sequence of coordinates and, together with the user identity stored in the user unit, may be forwarded via the mobile telephone 8 to the server unit 2. The server unit 2 may compare the received sequence of coordinates, i.e. the signature, with a sequence of coordinates stored earlier with the user identity. As used herein, when correspondence is detected the sequence of coordinate pairs are said to "favorably compare" with the stored sequence. If the received signature is determined to correspond, a signal may be sent to the computer 4 and the user is logged in.

[086] It is also possible to arrange the checking device in the computer 4, i.e. the access-protected unit.

[087] Another embodiment of the invention is similar to previous embodiments, but in this embodiment the user can log in to different physical entities by writing a command to select a log in and entity. The writing field 6 in this embodiment may be used to write a command associated with a physical entity, for example a computer. In this embodiment, the digital pen may have a unique identification code or PIN (Personal Identification Number). The identification code may be resident in the pen or user unit and may be used by the checking device which may also be located in the user unit. In an exemplary embodiment of the invention, the identification code may be a manufacturing number of the pen and may be hardcoded into the memory of the digital pen unable to be changed.

[088] The digital pen may be arranged to transfer the unique PIN and information generated by the user, to the server unit.

[089] In the memory of the server unit, information of the coordinate areas, commands and PINs may be stored.

[090] In a data structure in the memory of the server unit 2, information or rules for each coordinate area may be found which define how each coordinate area is to be processed.

[091] Fig. 5 shows an example of such a structure in table form. In a first column 40 of the table, the coordinate areas are defined with the aid of the coordinates (x1, y1; x2, y2) for determining the corners of the coordinate area which are assumed to be rectangular in this case. In a second column 41, a representation of a command associated with an access-protected unit, which is represented in column 42, is stored. In a fourth column 43, a PIN is stored so that the server unit 2 can compare a received

PIN with a PIN stored earlier. Naturally, this is a very simple structure which is only used for illustrating the principles of the invention. Considerably more complex structures and rules for security checking are conceivable within the scope of the invention.

[092] When a user wishes to obtain access to a computer 4. The user may place the digital pen 1 on the writing field 6 and the pen may register the pattern 7 and calculate corresponding coordinates. The user may write, for example, the command "comp" to log in to the computer. The pen may register the written command and calculate the relative corresponding coordinates. The pen may then forward the coordinates and the PIN of the digital pen 1 via the mobile phone 8 to the server unit 2. The server unit checks to determine to which coordinate area the registered coordinate belongs. Each user in the system may be associated with at least one coordinate area. The server unit may then check the command "comp" to determine which physical unit the user is logging in to. In Fig. 5, the command "comp" is associated with "Computer 23." Thereafter, it checks the PIN to determine if this pen in combination with the pattern 7 is allowed to have access to "Computer 23." If access is allowed, the server unit 2 may send a signal to "Computer 23" and the user is logged in.

Non-Recurrent Code

[093] A predetermined coordinate area on a writing base can also function as a non-recurrent field which, after having been used once, is used up. This can be applicable, by way of example only, when it is wished to be able to discard the writing base after use or when it is wished to keep it as a receipt for access to the system. It can be that the signature is also written on the base with ink, enabling an unauthorized

person to easily follow the written signature and in this way obtain unauthorized access to the access-protected unit. If, on the other hand, this pattern is used up, the only information remaining is the signature of the user.

Concurrently filed with the application for this patent are applications entitled Systems and Methods for Information Storage based on Swedish Application No. 0000947-2, filed March 21, 2000, and U.S. Provisional Application No. 60/207,839, filed May 30, 2000; Secured Access Using a Coordinate System based on Swedish Application No. 0000942-3, filed March 21, 2000, and U.S. Provisional Application No. 60/207,850 filed on May 30, 2000; System and Method for Printing by Using a Position Coding Pattern based on Swedish Application No. 0001245-0, filed on April 5, 2000, and U.S. Provisional Application No. 60/210,651, filed on June 9, 2000; Apparatus and Methods Relating to Image Coding based on Swedish Application No. 0000950-6, filed on March 21, 2000, and U.S. Provisional Application No. 60/207,838, filed on May 30, 2000; Apparatus and Methods for Determining Spatial Orientation based on Swedish Application No. 0000951-4, filed on March 21, 2000, and U.S. Provisional Application No. 60/207,844, filed on May 30, 2000; System and Method for Determining Positional Information based on Swedish Application No. 0000949-8, filed March 21, 2000, and U.S. Provisional Application No. 60/207,885, filed on May 30, 2000; Method and System for Transferring and Displaying Graphical Objects based on Swedish Application No. 0000941-5, filed March 21, 2000, and U.S. Provisional Application No. 60/208,165, filed May 31, 2000; Online Graphical Message Service based on Swedish Application No. 0000944-9, filed March 21, 2000, and U.S. Provisional Application No. 60/207,881, filed May 30, 2000; Method and System for Digitizing Freehand Graphics With User-

Selected Properties based on Swedish Application No. 0000945-6, filed March 21, 2000, U.S. Provisional Application No. 60/207,882, filed May 30, 2000; Data Form Having a Position-Coding Pattern Detectable by an Optical Sensor based on Swedish Application No. 0001236-9, filed April 5, 2000, and U.S. Provisional Application No. 60/208,167, filed May 31, 2000; Method and Apparatus for Managing Valuable Documents based on Swedish Application No. 0001252-6, filed April 5, 2000, and U.S. Provisional Application No. 60/210,653 filed June 9, 2000; Method and Apparatus for Information Management based on Swedish Application No. 0001253-4 filed April 5, 2000, and U.S. Provisional Application No. 60/210,652, filed June 9, 2000; Device and Method for Communication based on Swedish Application No. 0000940-7, filed March 21, 2000, and U.S. Provisional Application No. 60/208,166, filed May 31, 2000; Information-Related Devices and Methods based on Swedish Application No. 0001235-1, filed April 5, 2000, and U.S. Provisional Application No. 60/210,647, filed June 9, 2000; Processing of Documents based on Swedish Application No. 0000954-8, filed March 21, 2000, and U.S. Provisional Application No. 60/207,849, filed May 30, 2000; Secure Signature Checking System based on Swedish Application No. 0000943-1, filed March 21, 2000, and U.S. Provisional Application No. 60/207,880, filed May 30, 2000; Identification of Virtual Raster Pattern, based on Swedish Application No. 0001235-1, filed April 5, 2000, and U.S. Provisional Application No. 60/210,647, filed June 9, 2000, and Swedish Application No. 0004132-7, filed November 10, 2000, and U.S. Provisional Application No. _____, filed January 12, 2001; and a new U.S. Provisional Application entitled Communications Services Methods and Systems.

[094] The technical disclosures of each of the above-listed U.S. applications, U.S. provisional applications, and Swedish applications are hereby incorporated herein by reference. As used herein, the incorporation of a "technical disclosure" excludes incorporation of information characterizing the related art, or characterizing advantages or objects of this invention over the related art.

[095] In the foregoing Description of Preferred Embodiments, various features of the invention are grouped together in a single embodiment for purposes of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the following claims are hereby incorporated into this Description of the Preferred Embodiments, with each claim standing on its own as a separate preferred embodiment of the invention.